UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/801,115	03/16/2004	Koichi Tanimoto	62807-173	9181

20277 7590 08/16/2007
MCDERMOTT WILL & EMERY LLP
600 13TH STREET, N.W.
WASHINGTON, DC 20005-3096

EXAMINER	
TURCHEN, JAMES R	
ART UNIT	PAPER NUMBER
2139	
MAIL DATE	DELIVERY MODE
08/16/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/801,115	TANIMOTO ET AL.	
	Examiner	Art Unit	
	James Turchen	2139	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 March 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-9* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-9* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *16 March 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *09/11/06 & 08/08/05 & 03/16/04*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claims 1-9 are pending.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

1. Claims 1 and 4 are rejected under 35 U.S.C. 102(b) as being anticipated by Authentic Third-party Data Publication (hereinafter ATDP).

Regarding claim 1:

ATDP discloses a verification result recording method for creating a verification log recording information about verification of a signature in a signature system including a signer side apparatus, a verifier side apparatus and a publishing organization side apparatus, wherein:

said signer side apparatus records a signature log entry relating to a signature created as a signer side signature log with a chain relation (page 3 step 1, the owner (signer side) populates the relations in the database and computes the summary signatures of these data structures, signed with the owner's private key);

said publishing organization side apparatus publicizes said signature log entry deposited from said signer side apparatus, records a plurality of signature log entries deposited as a publishing organization side signature log with a chain relation and publicizes a predetermined signature log entry in said publishing organization side

signature log as a newspaper publication signature log entry (page 3 step 2, the owner distributes the summary signatures to clients and the database to the publishers and the publisher computes an answer q and a verification object in response to a client's (verifier side's) query; the verification object is based on a small number of summary signatures that are distributed periodically to the clients (verifier side) by the data owner (signer side) (page 2, Our Approach)); and

said verifier side apparatus verifies matching of the chain relation among said signatures from said newspaper publication signature log entry to said signature log entry deposited by said signer side apparatus for publication by using said publishing organization side signature log, verifies matching of the chain relation among said signatures from said signature log entry deposited by said signer side apparatus for publication to said signature log entry relating to said verification object signature by using said signer side signature log, and records the data used for said verification as a verification log (page 3 step 4, the client (verifier side) verifies the correctness and completeness of q by recomputing the summary signature using q, the verification object, and the public key; page 2 Our Approach, the verification object provides and unforgable proof which links the answer to the appropriate summary signature, which was already signed by the owner (signer side); the client records the summary signatures that are sent by the owner (thus creating a log of summary signatures)).

Regarding claim 4:

ATDP discloses a verifier side apparatus for executing signature verification, characterized by performing:

a reception processing for verifying a verification object signature by using a public key of a signer (page 3 step 1, the owner computes summary signatures, signed by the private key; it is inherent to verify the signature by decrypting with the signer's public key);

a verification processing for verifying a chain relation from a newspaper publication signature log entry as a starting point to said verification object signature by using a signer side signature log and a publishing organization side signature log (page 3 steps 2-4 and page 2, the verification object validates an answer set by providing an unforgable proof which links the answer to the appropriate summary signature; the summary signatures are bottom-up hashes computed recursively over B-tree type indexes for the entire set of tuples in each relation; the publisher uses the same B-tree structure to construct the verification object); and

a verification record preservation processing by creating a verification log from data used for said verification processing and recording said verification log (page 3 step 2, the client maintains the summary signatures (page 2 Our Approach, the owner periodically distributes the summary signatures), thus creating a log (a record or audit trail) of the summary signatures).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 2 and 3 are rejected under 35 U.S.C. 103(a) as being unpatentable over ATDP.

Regarding claim 2:

ATDP discloses the verification result recording method according to claim 1, but it does not disclose the contents of said log. The use of logs are well known in the art for recording events in a certain scope. One skilled in the art at the time of invention could have combined the method of ATDP with the method for using a log as it is known in the art in order to create an audit trail of transactions between the owner, the client, and the publisher.

Regarding claim 3:

ATDP discloses the verification result recording method according to claim 2, which includes the steps of:

extracting said verification object signature, said signer side signature log, said publishing organization side signature log and said newspaper publication signature log entry as the data utilized for said verification from said verification log (page 3 step 4, the client verifies the correctness and completeness; it is inherent that the client must pull information that it has previous received in order to verify the correctness of q, and the verification object);

verifying matching of the chain relation among said signatures from said newspaper publication signature log entry to said signature log entry relating to said verification object signature by utilizing said data utilized for said verification and so extracted (page 3 step 4, the client verifies the correctness and completeness; page 2

Our Approach, the summary signature and verification object are bottom-up hashes computed recursively (chain relation)); and

verifying said verification log (page 3 step 1, the summary signatures are signed by the owner and verified by the client using the public key of the owner).

3. Claims 5-9 are rejected under 35 U.S.C. 103(a) as being unpatentable over ATDP in view of Herald: Achieving a Global Event Notification Service (hereinafter Herald).

Regarding claim 5:

ATDP discloses a publishing organization side apparatus for executing a reliability improvement processing of a signature, characterized by performing:

a publication processing for publicizing a signature log entry deposited from a signer side apparatus (page 3 step 2, the owner publishes the summary signatures and the database to the publisher);

a publication reminder processing for urging said signer side apparatus to publicize said signature log entry (page 2 Our Approach, the owner distributes the summary signatures periodically to the clients);

a verification vicarious execution processing for verifying a verification object signature by collecting data necessary for verification in place of said signer side apparatus, creating a verification log and notifying a verification result (page 3 step 2, the signature summary and database is signed by the owner with the private key; verifying the owner is a matter of decrypting the information with the public key of the

signer; it is well known in the art that servers (publisher) keep a record of transactions for dispute resolution and locating problems as they arise).

ATDP does not disclose a reminder, however, reminders were well known in the art at the time of invention and one of ordinary skill in the art could have added a reminder to ATDP in order to ensure that the summary signatures are periodically distributed. ATDP discloses a distributed system of publishers, signers, and verifiers (page 2 Our Approach) but does not disclose a publication notice processing for notifying said signer side apparatus of publication of a signature log entry deposited from other signer side apparatus. Herald discloses an event notification system (Introduction). Herald additionally discloses event notification is a primary capability for building distributed applications (Introduction). It would have been obvious to one of ordinary skill in the art at the time of invention to modify the system of ATDP with the event notification system of Herald in order interconnect dynamically changing sets of clients and services (Introduction).

Regarding claim 6:

ATDP and Herald disclose the publishing organization side apparatus according to claim 5, which executes, as said publication processing:

a publication processing for publicizing a signature log entry deposited from said signer side apparatus for publication (page 3 step 2, the owner distributes the database to the publishers; it is well known for a publisher to publish information given to it);

a publication information registration processing for recording information relating to said signature log entry publicized (page 1 introduction, a financial markets database

(server) is accessed by clients; it is well known in the art for a server to record a log for audit trailing, dispute resolutions, intrusions, hardware failures, etc.);

a notice request existence/absence confirmation processing for confirming whether or not a publication notice request is received from other signer side apparatus as to said signature log entry publicized (page 1 introduction, a financial markets database (server) is accessed by clients ; it is well known in the art that in server/client communications to send an ACK/NACK packet in response to receiving information else the communication is considered faulty and/or timed out); and

a publication notice processing for giving a notice to said other signer side apparatus when said publication notice request is received as to said signature log entry publicized (Herald, page 90, section 3.3, delivery of an event notification message to many subscribers).

Regarding claim 7:

ATDP and Herald disclose the publishing organization side apparatus according to claim 5, but do not disclose wherein said publication reminder processing executes:

Reminders were well known in the art at the time of invention and one of ordinary skill in the art could have added a reminder to ATDP in order to ensure that the summary signatures are periodically distributed. Adding reminders to the system of ATDP and Herald would allow for:

an object extraction processing for specifying a signer to which publication of said signature log entry is to be urged wherein a reminder transmission processing for transmitting a reminder document urging publication of said signature log entry to said

signer side apparatus utilized by said signer specified (page 2 Our Approach, the summary signatures are distributed periodically; it is obvious that the reminder is sent to the owner that needs to be reminded to publish); and

a reminder information registration processing for recording transmission of said reminder document (page 1 introduction, a financial markets database (server) is accessed by clients; it is well known in the art for a server to record a log for audit trailing, dispute resolutions, intrusions, hardware failures, etc.; it would be obvious to record the reminder information processing as a result of sending out the reminder).

Regarding claim 8:

ATDP and Herald disclose the publishing organization side apparatus according to claim 5, wherein said publication notice processing executes:

a notice request content registration processing for receiving said publication notice request from said other signer side apparatus and registering the content of said publication notice request to said database (page 3 step 1, the owner populates relations in the database and distributes the database to publishers; it is obvious that an owner gets permission to publish beforehand);

a notice requesting party extraction processing for extracting information of said other signer side apparatus as a notice requesting party from said database registering the content of said notice request content (page 3 steps 1-4, the data is sent to the publisher and the publisher provides the data for the client; it is inherent that the publisher extract and store the information being sent to be published); and

a notice transmission processing for notifying said other signer side apparatus as said notice requesting party of publication of said publication signature log entry by said notice requesting object signer (page 1 introduction, a financial markets database (server) is accessed by clients; it is well known in the art that a server side apparatus confirms that the service requested has been processed).

Regarding claim 9:

ATDP and Herald disclose the publishing organization side apparatus according to claim 5, wherein said verification vicarious execution processing executes:

a verification vicarious execution request reception processing for receiving a request of verification vicarious execution from said signer side apparatus (page 3, the data is signed with the private key);

a verification data collection processing for collecting a publication signature log entry and a signature log necessary for verification for said verification signature for which verification is requested. ATDP or Herald does not explicitly state retrieving a key, however, it would have been obvious to one of ordinary skill in the art at the time of invention to retrieve the public key of the owner from a list of public keys in order to decrypt the contents signed by the private key (page 3 step 2, owner signs data with the private key);

a signature verification processing for verifying said verification signature for which verification is requested, by using the data collected by said verification data collection processing (page 3 step 2, the owner distributes the database, signed by the private key, to the publisher; it is inherent that the publisher decrypt the database using

the owner's public key and by decrypting the data using the owner's public key, the publisher verifies the owner);

a verification log creation processing for creating a verification log recording said verification result and the data used for said verification and sending said verification log to said signer side apparatus as a verification requesting party (page 3 steps 1-4; the owner provides the publisher the data and the publisher provides the client with the data; the publisher is acting as a server side apparatus for both the owner and the client; it is inherent for a server side apparatus confirms that a requested service has been performed or processed);

a verification status registration processing for recording a verification status to said database for said verification object signature requested (page 3 steps 1-4; the owner provides the publisher the data and the publisher provides the client with the data; the publisher is acting as a server side apparatus for both the owner and the client; it is well known in the art for a server side apparatus to record information that has taken place as to provide fault recovery, audit trails, dispute resolution, etc.); and

a verification status confirmation processing for confirming said verification status for said verification vicarious execution processing requested (page 3 step 2, the owner distributes the database, signed by the private key, to the publisher; it is inherent that the publisher decrypt the database using the owner's public key and by decrypting the data using the owner's public key, the publisher verifies the owner; after verifying the owner, it is inherent to update the owner's verification status with the publisher (as in the data was verified as coming from the owner)).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to James Turchen whose telephone number is 571-270-1378. The examiner can normally be reached on MTWRF 7:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571)272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

JRT

CHRISTOPHER REVAK
PRIMARY EXAMINER